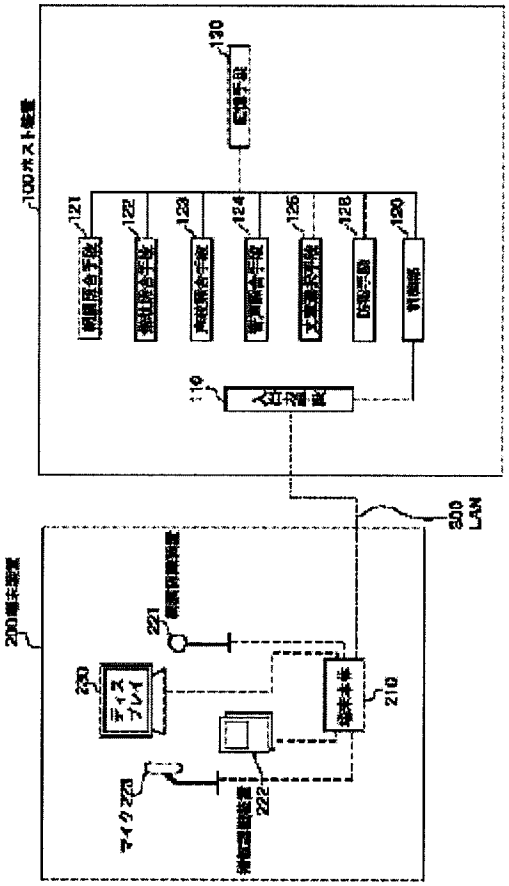
ELECTRONIC APPROVAL SYSTEM AND METHOD USING INDIVIDUAL IDENTIFICATION

Publication number: JP2001195364
Publication date: 2001-07-19
Inventor: UCHIDA KAZUYOSHI
Applicant: NEC INFORMATION SERVICE LTD
Classification:
- international: ***G06F21/20; G06F15/00;*** **G06F21/20; G06F15/00;** (IPC1-7): G06F15/00
- European:
Application number: JP20000002625 20000111
Priority number(s): JP20000002625 20000111

Abstract of **JP2001195364**

PROBLEM TO BE SOLVED: To provide an electronic approval system and an electronic approval method for surely preventing the participation of anyone other than the individual by combining many kinds of individual identification/security functions. SOLUTION: This system is constituted of a host device 100 and terminal equipment 200 connected by a LAN 300. The host device 100 is provided with an input/output means 110, a control part 120, a storage means 130, a retina collation means 121, a fingerprint collation means 122, a sentence selection means 125, a voiceprint collation means 123 for collating the voiceprint information with the preserved voiceprint information of the individual based on voice information for which the individual reads a selected sentence aloud, a voice collation means 124 for collating voice contents with the selected sentence and judging a burglar prevention keyword further and a burglar prevention means 126 for operating a burglar preventing operation by the judgment of the voice collation means 124. The terminal equipment 200 is provided with a terminal main body 210, a retina recognition device 221, a fingerprint recognition device 222, a microphone 223 and a display 230.



Family list
2 family member for: **JP2001195364**
Derived from 1 application

Back to JP2001195

1 **ELECTRONIC APPROVAL SYSTEM AND METHOD USING INDIVIDUAL IDENTIFICATION**

Inventor: UCHIDA KAZUYOSHI

Applicant: NEC INFORMATION SERVICE LTD

EC:

IPC: ***G06F21/20; G06F15/00***; **G06F21/20** (+2)

Publication info: **JP3538095B2 B2** - 2004-06-14
JP2001195364 A - 2001-07-19

Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－195364
（P2001－195364A）
(43)公開日　平成13年７月19日(2001.7.19)

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　15/00	３３０	Ｃ０６Ｆ　15/00	３３０Ｆ　５Ｂ０８５

審査請求　有　　請求項の数８　ＯＬ　（全 10 頁）

(21)出願番号　特願2000－2625(P2000－2625)

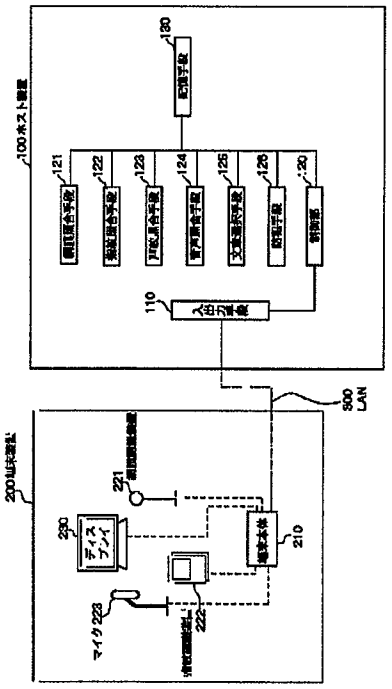
(22)出願日　平成12年１月11日(2000.1.11)

(71)出願人　390001041
日本電気情報サービス株式会社
東京都港区三田１丁目４番28号
(72)発明者　内田　和義
東京都港区三田一丁目４番28号　日本電気情報サービス株式会社内
(74)代理人　100088328
弁理士　金田　暢之　（外２名）

Ｆターム(参考)　5B085 AE23 AE25 AE26 AE27

(54)【発明の名称】　個人識別を用いた電子承認システムおよび方法

(57)【要約】
【課題】　多種類の個人識別・セキュリティ機能を組み合わせることによって該当個人以外の関与を確実に防止する電子承認システムと電子承認方法を提供する。
【解決手段】　ＬＡＮ３００により接続されたホスト装置１００と端末装置２００とから構成され、ホスト装置１００は、入出力手段１１０と、制御部１２０と、記憶手段１３０と、網膜照合手段１２１と、指紋照合手段１２２と、文章選択手段１２５と、選択された文章を個人が音読した音声情報をもとにその声紋情報を保存された個人の声紋情報と照合する声紋照合手段１２３と、音声内容を選択された文章と照合し、さらに防犯キーワードを判定する音声照合手段１２４と、音声照合手段１２４の判定により防犯動作を作動させる防犯手段１２６とを備え、端末装置２００は端末本体２１０と、網膜認識装置２２１と、指紋認識装置２２２と、マイク２２３と、ディスプレイ２３０とを備える。



【特許請求の範囲】
【請求項１】　ＬＡＮにより接続されたホスト装置と端末装置とから構成され、
前記ホスト装置は、外部との情報の入出力を行う入出力手段と、入力情報に基づいて所定の手順で各種の処理を行い結果を外部に出力する制御部と、個人情報を含む情報を保存する記憶手段と、入力した網膜情報を前記記憶手段に保存された網膜情報と照合する網膜照合手段と、入力した指紋情報を前記記憶手段に保存された指紋情報と照合する指紋照合手段と、前記記憶手段に保存された文章から文章を選択する文章選択手段と、選択された前記文章を個人が音読した音声情報をもとにその声紋情報を前記記憶手段に保存された声紋情報と照合する声紋照合手段と、音声内容を選択された前記文章と照合する音声照合手段と、を備え、
前記端末装置は、ＣＰＵを有して入出力を担当し、網膜情報，指紋情報，音声情報を含む情報を収集してホスト装置に情報を送信し、ホスト装置からの情報を受信する端末本体と、認証時に使用される生活反応検知付き網膜認識の入力に使用される網膜認識装置と、承認時に使用される指紋認識の入力に使用される指紋認識装置と、承認の最終確認で使用される音声を入力するマイクと、電子承認の各工程を進めるためのメッセージおよび警告メッセージを出力するために使用されるディスプレイと、を備えることを特徴とする個人識別を用いた電子承認システム。
【請求項２】　前記ホスト装置の音声照合手段は、また、音声内容に含まれる防犯キーワードを判定し、前記ホスト装置は、さらに、前記音声照合手段の判定により防犯動作を作動させる防犯手段を備え、
前記端末装置のマイクは、防犯機能で使用される音声も入力される、請求項１に記載の個人識別を用いた電子承認システム。
【請求項３】　前記ホスト装置内にも前記端末装置が組み込まれている、請求項１または請求項２に記載の個人識別を用いた電子承認システム。
【請求項４】　記録媒体を備え、前記制御部の動作は、記録媒体に記録された個人識別を用いた電子承認プログラムにより制御できる、請求項１から請求項３のいずれか１項に記載の個人識別を用いた電子承認システム。
【請求項５】　端末装置の網膜認識装置から入力された網膜情報、指紋認識装置から入力された指紋情報、およびマイクから入力された音声情報をもとに、入力した該当個人を認証し、承認確認項目ごとに承認を確認し、承認を最終確認するための個人識別を用いた電子承認方法であって、
該当個人を認証するために、前記網膜認識装置から入力した該当個人の網膜情報を記憶手段に保存された個人情報と照合して、該当個人の網膜であることを確認するステップと、
該当個人を認証するために、前記網膜認識装置から入力した該当個人の網膜情報から生活反応の有無を確認するステップと、
承認確認項目毎の承認を行うために、承認確認項目毎に前記指紋認識装置から入力した該当個人の指紋情報を記憶手段に保存された個人情報と照合して、該当個人の指紋であることを確認するステップと、
承認の最終確認のために、すべての承認確認項目の承認が終了すると、記憶手段に保存されている文章の中から所定の手順で最終承認用文章を選択し、端末装置のディスプレイに表示するステップと、
該当個人が前記マイクに向かって表示された文章を音読した音声の声紋情報を記憶手段に保存された個人情報と照合して、該当個人の声紋であることを確認するステップと、
該当個人が前記マイクに向かって表示された文章を音読した音声の音声情報を選択された前記最終承認用文章と照合して、音声が最終承認用文章であることを確認するステップと、
承認の最終確認のための声紋と音声とが確認されると、承認の最終確認が成功したものとして承認時に承認した電子承認をすべて完了させるステップと、を備えたことを特徴とする個人識別を用いた電子承認方法。
【請求項６】　上記の各ステップに加えて、
認証から承認の最終確認までの間、前記マイクと音声照合手段とを待機状態とさせ、前記マイクから入力された音声を記憶手段に保存されている予め登録された防犯キーワードと照合し、音声が防犯キーワードであった場合、管理者への通知を行って所定の防犯動作を作動させるステップと、
承認の最終確認のための声紋と音声とが確認された場合には、承認時に承認した電子承認をすべて完了させるステップの代わりに、最終承認の成功メッセージを前記端末装置に送信してディスプレイに表示するステップと、
防犯動作が作動中か否かの確認を行って、防犯動作が作動していなければ、承認の最終確認が成功したものとして承認時に承認した電子承認をすべて完了させるステップと、を備えた請求項５に記載の個人識別を用いた電子承認方法。
【請求項７】　端末装置の網膜認識装置から入力された網膜情報、指紋認識装置から入力された指紋情報、およびマイクから入力された音声情報をもとに、入力した該当個人を認証し、承認確認項目ごとに承認を確認し、承認を最終確認するための制御プログラムを記録した記録媒体であって、
該当個人を認証するために、前記網膜認識装置から入力した該当個人の網膜情報を網膜照合手段により記憶手段の個人情報と照合して、該当個人の網膜であることを確認する手順と、
該当個人を認証するために、前記網膜認識装置から入力

した該当個人の網膜情報から前記網膜照合手段により生活反応の有無を確認する手順と、
承認確認項目毎の承認を行うために、承認確認項目毎に前記指紋認識装置から入力した該当個人の指紋情報を指紋照合手段により記憶手段の個人情報と照合して、該当個人の指紋であることを確認する手順と、
承認の最終確認のために、すべての承認確認項目の承認が終了すると、文章選択手段により記憶手段に保存されている文章の中から所定の手順で最終承認用文章を選択し、端末装置に送信して端末装置のディスプレイに表示する手順と、
該当個人が前記マイクに向かって表示された文章を音読した音声の声紋情報を声紋照合手段で記憶手段の個人情報と照合して、該当個人の声紋であることを確認する手順と、
該当個人が前記マイクに向かって表示された文章を音読した音声の音声情報を音声照合手段で前記文章選択手段で選択された最終承認用文章と照合して、音声が最終承認用文章であることを確認する手順と、
承認の最終確認のための声紋と音声とが確認されると、承認の最終確認が成功したものとして承認時に承認した電子承認をすべて完了させる手順と、を実行させるためのプログラムを記録した機械読み取り可能な記録媒体。
【請求項８】　上記の各手順に加えて、
認証から承認の最終確認までの間、前記マイクと音声照合手段とを待機状態とさせ、音声照合手段で、端末装置の前記マイクから入力された音声を記憶手段に保存されている予め登録された防犯キーワードと照合させ、音声が防犯キーワードであった場合、管理者への通知を行って所定の防犯動作を作動させる手順と、
承認の最終確認のための声紋と音声とが確認されるた場合には、承認時に承認した電子承認をすべて完了させる手順の代わりに、最終承認の成功メッセージを前記端末装置に送信してディスプレイに表示する手順と、
防犯手段で防犯動作が作動中か否かの確認を行って、防犯動作が作動していなければ、承認の最終確認が成功したものとして承認時に承認した電子承認をすべて完了させる手順と、を実行させるためのプログラムを記録した請求項７に記載の機械読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は電子承認システムに関し、特にセキュリティを強化した電子承認システムに関する。
【０００２】
【従来の技術】近年インターネット等の通信回線を利用したエレクトロニック・コマースの普及に伴って、セキュリティ確保のために、ネットワーク上の個人や法人が確かに本人であることを確認する電子認証や、本人の意思により発行された書類であることを確認する電子承認の必要性が高まってきた。このためネットワーク上で電子化されたユーザＩＤやパスワードなどの電子化されたデータを用いて本人を確認する方法が用いられたり、証明書を発行するだけの信頼に足る第三者機関を含む認証システムとデータのセキュリティを保証するための暗号システムが求められている。
【０００３】
【発明が解決しようとする課題】しかしながら、ユーザＩＤやパスワードなどを用いた従来の個人認証においては、そのユーザＩＤやパスワードなどが盗まれて用いられた場合にはそれを防ぐ方法がなく、セキュリティのレベルを上げるために指紋承認を用いた場合においても次のような課題がある。
【０００４】その第１の課題は、脅迫などの犯罪行為によって入力された指紋をリアルタイムに検知できないということであり、第２の課題は、指紋承認などで遺体の腕を切断して使用する場合の不正な認証を検知できないということである。
【０００５】本発明の目的は、網膜認識，指紋認識，声紋認識および音声認識の４種類の個人識別・セキュリティ機能を組み合わせることによって該当個人以外の関与を確実に防止する電子承認システムを提供することにある。
【０００６】
【課題を解決するための手段】本発明の個人識別を用いた電子承認システムは、ＬＡＮにより接続されたホスト装置と端末装置とから構成され、ホスト装置は、外部との情報の入出力を行う入出力手段と、入力情報に基づいて所定の手順で各種の処理を行い結果を外部に出力する制御部と、個人情報を含む情報を保存する記憶手段と、入力した網膜情報を記憶手段に保存された網膜情報と照合する網膜照合手段と、入力した指紋情報を記憶手段に保存された指紋情報と照合する指紋照合手段と、記憶手段に保存された文章から文章を選択する文章選択手段と、選択された文章を個人が音読した音声情報をもとにその声紋情報を記憶手段に保存された声紋情報と照合する声紋照合手段と、音声内容を選択された文章と照合する音声照合手段とを備え、端末装置は、ＣＰＵを有して入出力を担当し、網膜情報，指紋情報，音声情報を含む情報を収集してホスト装置に情報を送信し、ホスト装置からの情報を受信する端末本体と、認証時に使用される生活反応検知付き網膜認識の入力に使用される網膜認識装置と、承認時に使用される指紋認識の入力に使用される指紋認識装置と、承認の最終確認で使用される音声を入力するマイクと、電子承認の各工程を進めるためのメッセージおよび警告メッセージを出力するために使用されるディスプレイとを備えている。
【０００７】ホスト装置の音声照合手段は、また、音声内容に含まれる防犯キーワードを判定し、ホスト装置は、さらに、音声照合手段の判定により防犯動作を作動

させる防犯手段を備え、端末装置のマイクは、防犯機能で使用される音声も入力されるシステムであってもよい。

【０００８】また、ホスト装置内にも端末装置が組み込まれていてもよく、記録媒体を備え、制御部の動作は、記録媒体に記録された個人識別を用いた電子承認プログラムにより制御できてもよい。

【０００９】本発明の個人識別を用いた電子承認方法は、端末装置の網膜認識装置から入力された網膜情報、指紋認識装置から入力された指紋情報、およびマイクから入力された音声情報をもとに、入力した該当個人を認証し、承認確認項目ごとに承認を確認し、承認を最終確認するための個人識別を用いた電子承認方法であって、該当個人を認証するために、網膜認識装置から入力した該当個人の網膜情報を記憶手段に保存された個人情報と照合して、該当個人の網膜であることを確認するステップと、該当個人を認証するために、網膜認識装置から入力した該当個人の網膜情報から生活反応の有無を確認するステップと、承認確認項目毎の承認を行うために、承認確認項目毎に指紋認識装置から入力した該当個人の指紋情報を記憶手段に保存された個人情報と照合して、該当個人の指紋であることを確認するステップと、承認の最終確認のために、すべての承認確認項目の承認が終了すると、記憶手段に保存されている文章の中から所定の手順で最終承認用文章を選択し、端末装置のディスプレイに表示するステップと、該当個人がマイクに向かって表示された文章を音読した音声の声紋情報を記憶手段に保存された個人情報と照合して、該当個人の声紋であることを確認するステップと、該当個人がマイクに向かって表示された文章を音読した音声の音声情報を選択された最終承認用文章と照合して、音声が最終承認用文章であることを確認するステップと、承認の最終確認のための声紋と音声とが確認されると、承認の最終確認が成功したものとして承認時に承認した電子承認をすべて完了させるステップと、を備えている。

【００１０】上記の各ステップに加えて、認証から承認の最終確認までの間、マイクと音声照合手段とを待機状態とさせ、マイクから入力された音声を記憶手段に保存されている予め登録された防犯キーワードと照合し、音声が防犯キーワードであった場合、管理者への通知を行って所定の防犯動作を作動させるステップと、承認の最終確認のための声紋と音声とが確認された場合には、承認時に承認した電子承認をすべて完了させるステップの代わりに、最終承認の成功メッセージを端末装置に送信してディスプレイに表示するステップと、防犯動作が作動中か否かの確認を行って、防犯動作が作動していなければ、承認の最終確認が成功したものとして承認時に承認した電子承認をすべて完了させるステップと、を備えていてもよい。

【００１１】本発明は、電子承認システムに用いられる個人識別において、４種類（網膜認識，指紋認識，声紋認識および音声認識）の個人識別・セキュリティ機能を用いることによって、該当個人以外の関与による承認を確実に防止することを特徴としている。このため、行政等における機密情報の電子承認にも利用可能である。ここで認証時には、網膜認識を用いて、該当個人と認識するとともに、生活反応の有無を確認し、承認時には指紋認識を用いて、該当個人の意思による承認と認識し、承認の最終確認時には声紋認識と音声認識を用いて、該当個人以外の操作を不可能にしている。

【００１２】さらに防犯のためには音声認識を用いた「防犯キーワード認識によるセキュリティ機能」を使用し、該当個人以外の関与を防止している。

【００１３】このようにして、本願発明では電子承認システムにおけるセキュリティ機能を強化して該当個人以外の関与を不可能にしているので、電子承認システムにおいて確実に防犯を実現できる。

【００１４】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。図１は本発明の第１の実施の形態の個人識別を用いた電子承認システムの模式的ブロック構成図である。

【００１５】本発明の第１の実施の形態の個人識別を用いた電子承認システムはＬＡＮ３００により接続されたホスト装置１００と端末装置２００とから構成される。図１では端末装置２００は１組として表示されているが複数の端末装置２００がＬＡＮ３００によりホスト装置１００と接続されていてもよい。

【００１６】ホスト装置１００は、端末装置などの外部との情報の入出力を行う入出力手段１１０と、入力情報に基づいて所定の手順で各種の処理を行い結果を外部に出力する制御部１２０と、記憶手段１３０と、入力した網膜情報を記憶手段１３０に保存された網膜情報と照合する網膜照合手段１２１と、入力した指紋情報を記憶手段１３０に保存された指紋情報と照合する指紋照合手段１２２と、記憶手段１３０に保存された文章から文章を選択する文章選択手段１２５と、選択された文章を個人が音読した音声情報をもとにその声紋情報を記憶手段１３０に保存された声紋情報と照合する声紋照合手段１２３と、音声内容を選択された文章と照合し、さらに防犯キーワードを判定する音声照合手段１２４と、音声照合手段１２４の判定により防犯動作を作動させる防犯手段１２６とを備える。

【００１７】ホスト装置１００は、端末装置２００で該当個人から入力された情報を基に個人情報の照合や防犯キーワードの認識を行い、端末装置２００に対して電子承認の各工程を進めるためのメッセージおよび警告メッセージを送信する。このように個人情報を一元的に管理するため、ホスト側の記憶手段１３０には個人情報が格納されている。

【００１８】端末装置２００は、ＣＰＵを有して入出力を担当し、網膜情報，指紋情報，音声情報等を収集してホスト装置１００に情報を送信し、ホスト装置１００からの情報を受信する端末本体２１０と、認証時に使用する「生活反応検知付き網膜認識機能」に使用される網膜情報を入力する網膜認識装置２２１と、承認時に使用する指紋認識に使用される指紋を入力する指紋認識装置２２２と、承認の最終確認および防犯機能で使用される音声を入力するマイク２２３と、電子承認の各工程を進めるためのメッセージおよび警告メッセージを出力するために使用されるディスプレイ２３０とを備える。

【００１９】本発明では、電子承認システムに用いられる個人識別において、４種類（網膜認識，指紋認識，声紋認識および音声認識）の個人識別・セキュリティ機能を用いており、（１）認証時・・・網膜認識を用いて、該当個人と認識し、（２）承認時・・・指紋認識を用いて、該当個人の意思による承認と認識し、（３）承認の最終確認時・・・声紋認識と音声認識とを用いて、該当個人以外の操作を不可能にするので、該当個人以外の関与による承認を確実に防止できることを特徴としている。このため、行政等における機密情報の電子承認にも利用可能である。また、（４）防犯・・・音声認識を用いた「防犯キーワード認識によるセキュリティ機能（以下、防犯機能と表記する場合あり）」を使用することにより、該当個人以外の関与が防止できる。

【００２０】以上の（１）～（４）を組み合わせた電子承認システムとなっているので、電子承認システムにおけるセキュリティ機能が強化され該当個人以外の関与を不可能にしており、電子承認システムにおいて防犯を確実に実現できる。

【００２１】以上の（１）～（４）を更に詳細に説明すると、

（１）認証時の個人照合および入力には「生活反応検知付き網膜認識機能」が用いられる。これは、網膜認識装置２２１による網膜認識時に瞳孔の伸縮による生活反応も確認することによって、本人が殺害されている場合の認証を不可能にし、該当個人以外の関与を防ぐことができる。

（２）承認時の個人照合および入力には指紋認識が用いられる。指紋照合機能１２２による指紋照合により、本人が端末装置２００の前に着席していることが確認されるので、該当個人の意思のもとで承認していることを確実に認識することができる。

（３）全ての承認の最終確認の個人照合および入力には声紋認識と音声認識を用いた「文章音声入力による個人生存判定機能」が採用されている。これは、最終承認を行うために、文章選択手段１２５により選択され端末装置２００のディスプレイ２３０に表示された文章を該当個人がマイク２２３によって入力すると、ホスト装置１００の声紋認識手段１２３と音声認識手段１２４とによって該当個人による音声入力であることを確認し、該当個人の意思のもとで行われた承認であることをさらに確実に認識することができる。採用する文章には新聞などの時事や抑揚の出やすい文章を採用し、週または月単位で変更する。認識の精度（サンプリングレート）を上げることによってデジタル音声入力を検知し、音声合成による入力を不可能にしている。また、「文章音声入力による個人生存判定機能」によって、テープ等に録音された該当個人の肉声やサンプリング（デジタル音声化）された音声合成による入力を不可能にしている。さらに、

（４）上記（１）～（３）の全工程において銃器・刃物等を用いた脅迫時の該当個人の承認を防ぐために、音声認識を用いた「防犯キーワード認識によるセキュリティ機能」が採用されている。これは、防犯キーワードがマイクによって入力されたことが音声認識で確認された場合、管理者に通知して最終的に承認を無効にする機能である。例えば、防犯キーワードを「テスト、テスト」にすると（３）の最終確認前のマイク動作確認時に、通常の振る舞いで該当個人が入力できて防犯措置を行うことができる。防犯キーワードは複数指定可能にして状況に対応した選択を可能とし、マイクは常時入力可能な状態にしておくことにより本人が防犯キーワードを入力する機会が拡大する。防犯キーワードの受信によりホスト装置１００の防犯機能手段１２６が作動した場合でも全工程終了後、端末装置２００のディスプレイ２３０には正常終了メッセージを表示し、通常承認時と同様の動作を行い、脅迫者に防犯機能手段１２６が作動したことを悟られないようにする。この防犯機能は（ａ）犯罪を検知し、（ｂ）脅迫者から該当個人の生命を守り、併せて（ｃ）該当個人以外の関与を検知・防止することを目的としている。

【００２２】次に、本発明の第１の実施の形態の個人識別を用いた電子承認システムの動作について図面を参照して説明する。電子承認は、認証→承認→承認の最終確認の順に行われ、図２は認証時の各ステップを表すフローチャートであり、図３は承認時の各ステップを表すフローチャートであり、図４は承認の最終確認時の各ステップを表すフローチャートである。

【００２３】認証時には、図２に示すように認証を開始すると（Ｓ１０１）、端末装置２００のディスプレイ２３０の表示にしたがって該当個人は網膜認識装置２２１から網膜情報を入力し、ホスト装置１００の網膜照合手段１２１は入力された網膜情報を記憶手段１３０の個人情報と照合し（Ｓ１０２）、該当個人の網膜であることが確認されると（Ｓ１０２Ｙ）、生活反応の有無を確認し（Ｓ１０３）、生活反応がある場合は（Ｓ１０３Ｙ）、認証成功として次の承認に進み（Ｓ１０４）、認証を終了する（Ｓ１０６）。該当個人の網膜でない場合と（Ｓ１０２Ｎ）、生活反応がない場合とは（Ｓ１０３Ｎ）、認証失敗として（Ｓ１０５）、認証を終了する

（Ｓ１０６）。

【００２４】承認時には、図３に示すように承認を開始すると（Ｓ２０１）、承認確認項目毎に端末装置２００のディスプレイ２３０の表示にしたがって該当個人は指紋認識装置２２２から指紋情報を入力し、ホスト装置１００の指紋照合手段１２２は入力された指紋情報を記憶手段１３０の個人情報と照合し（Ｓ２０２）、該当個人の指紋であることが確認されると（Ｓ２０２Ｙ）、承認成功として次の承認の最終確認の入力待ちとなって（Ｓ２０３）、承認を終了する（Ｓ０５）。該当個人の指紋でない場合は（Ｓ２０２Ｎ）、承認失敗として承認確認項目の承認を認めないで（Ｓ２０４）、承認を終了する（Ｓ２０５）。

【００２５】承認の最終確認時では、図４に示すように、すべての承認確認項目の承認が終了すると承認の最終確認を開始し（Ｓ３０１）、ホスト装置１００の文章選択手段１２５により記憶手段１３０に保存されている文章の中から所定の手順で最終承認用文章を選択し、端末装置２００に送信し、端末装置２００のディスプレイ２３０に表示する（Ｓ３０１）。次に該当個人はマイク２２３に向かって表示された文章を音読し、ホスト装置１００では端末装置２００から入力された音声情報をもとに、先ず声紋照合手段１２３で記憶手段１３０の個人情報と照合し（Ｓ３０３）、該当個人の声紋であることが確認されると（Ｓ３０３Ｙ）、続いて、音声照合手段１２４で文章選択手段１２５で選択された最終承認用文章と照合し（Ｓ３０４）、音声が最終承認用文章であることが確認されると（Ｓ３０４Ｙ）、最終承認の成功メッセージを端末装置２００に送信しディスプレイ２３０に表示する（Ｓ３０５）。次に防犯手段１２６で防犯動作が作動中か否かの確認を行い（Ｓ３０６）、防犯動作が作動していなければ（Ｓ３０６Ｎ）、承認の最終確認が成功したものとして承認時に承認した電子承認をすべて完了して（Ｓ３０７）、承認の最終確認を終了する（Ｓ３１０）。防犯動作が作動中の場合は（Ｓ３０６Ｙ）は承認の最終確認が失敗したものとして電子承認を全て無効にして（Ｓ３０９）、承認の最終確認を終了する（Ｓ３１０）。該当個人の声紋でない場合と（Ｓ３０３Ｎ）、音声が最終承認用文章でない場合とは（Ｓ３０４Ｎ）、不正使用として管理者へ通知を行い（Ｓ３０８）、承認の最終確認が失敗したものとして電子承認を全て無効にして（Ｓ３０９）、承認の最終確認を終了する（Ｓ３１０）。

【００２６】図５は防犯時の各ステップを表すフローチャートであり、防犯は、認証から承認の最終確認までの間、常に音声入力を待機する状態で行われる。防犯機能が開始されると（Ｓ４０１）、マイク２２３と音声照合手段１２４が待機状態となり（Ｓ４０２）、端末装置２００のマイク２２３から入力された音声は、ホスト装置１００に送られ、音声照合手段１２４で、記憶手段１３０に保存されている予め登録された防犯キーワードと照合され、防犯キーワードの確認が行われる（Ｓ４０３）。音声が防犯キーワードであった場合（Ｓ４０３Ｙ）、管理者への通知を行って（Ｓ４０４）、所定の防犯動作を作動させて（Ｓ４０５）、ステップＳ４０２に戻り音声入力を待機する。音声が防犯キーワードでない場合は（Ｓ４０３Ｎ）、防犯機能終了であるかを確認し（Ｓ４０６）、終了でない場合は（Ｓ４０６Ｎ）、ステップＳ４０２に戻り音声入力を待機する。終了の場合は（Ｓ４０６Ｙ）防犯機能を終了する（Ｓ４０７）。

【００２７】これまでの説明では防犯機能を組み込んだ状態で説明したが、防犯機能を除いたシステムと方法としても高いセキュリティ機能を得ることができる。

【００２８】また、本発明の第１の実施の形態ではホスト装置１００と端末装置２００はＬＡＮで接続された状態で説明したが、ホスト装置１００の内部にも端末装置２００を組み込むことも可能である。

【００２９】また、第１の実施の形態では電子文書における該当個人の認証、承認、承認の最終確認を前提に説明したが、この個人識別を用いた電子承認システムおよび電子承認方法の対象は電子文書に限定されるものではない。第１の実施の形態の承認の最終確認の個人照合および入力に使用した声紋認識と音声認識を用いた「文章音声入力による個人生存判定機能」と「防犯キーワード認識によるセキュリティ機能」の他の使用法を説明する。

【００３０】例えば、機密管理された部屋への入室のために網膜照合や指紋照合を使用する場合には、殺害された該当個人の遺体の一部（例えば指紋）を使用して入室が可能である。ここに「文章音声入力による個人生存判定機能」と「防犯キーワード認識によるセキュリティ機能」を組み合わせて使用すれば、脅迫による入室も含め、不正入室を防ぐことができる。このシステムは本発明の第１の実施の形態で説明した個人識別を用いた電子承認システムおよび電子承認方法をそのまま適用できる。

【００３１】このように、「文章音声入力による個人生存判定機能」と「防犯キーワード認識によるセキュリティ機能」とを組み合わせて使用すれば、（１）生存している該当個人の照合をより確実にし、（２）あらゆる不正入室を検知および防止する効果を得られる。

【００３２】次に、本発明の第２の実施の形態の個人識別を用いた電子承認システムと電子承認方法について図面を参照して説明する。図６は本発明の第２の実施の形態の個人識別を用いた電子承認システムの模式的ブロック構成図である。

【００３３】図６は、本発明のホスト装置１００を、装置を構成するコンピュータとして示したものであり、コンピュータはモデム、キーボード、ポインティングデバイス等の入力部１０１、モデム、プリンタ、ディスプレ

イ等の出力部１０２、データ処理装置１０３、記憶部１０４および記録媒体１０５を備える。記録媒体１０５には各部の動作を制御できる本発明の個人識別を用いた電子承認システム制御プログラムが記録されており、ＦＤ，ＣＤ－ＲＯＭ、半導体メモリ等が用いられる。

【００３４】個人識別を用いた電子承認システムの構成や個人識別を用いた電子承認方法は第１の実施の形態と同じなので説明を省略する。

【００３５】端末装置２００の網膜認識装置２２１から入力された網膜情報、指紋認識装置２２２から入力された指紋情報、およびマイク２２３から入力された音声情報をもとに、入力した該当個人を認証し、承認確認項目ごとに承認を確認し、承認を最終確認するための制御プログラムは、記録媒体１０５からデータ処理装置１０３に読み込まれデータ処理装置１０３の動作を制御する。データ処理装置１０３は制御プログラムの制御により以下の処理を実行する。

【００３６】即ち、認証から承認の最終確認までの間、マイク２２３と音声照合手段１２４とを待機状態とさせ、音声照合手段１２４で、端末装置２００のマイク２２３から入力された音声を記憶手段１３０に保存されている予め登録された防犯キーワードと照合させ、音声が防犯キーワードであった場合、管理者への通知を行って所定の防犯動作を作動させる処理と、該当個人を認証するために、網膜認識装置２２１から入力した該当個人の網膜情報を網膜照合手段１２１により記憶手段１３０の個人情報と照合して、該当個人の網膜であることを確認する処理と、該当個人を認証するために、網膜認識装置２２１から入力した該当個人の網膜情報から網膜照合手段１２１により生活反応の有無を確認する処理と、承認確認項目毎の承認を行うために、承認確認項目毎に指紋認識装置２２２から入力した該当個人の指紋情報を指紋照合手段１２２により記憶手段１３０の個人情報と照合して、該当個人の指紋であることを確認する処理と、承認の最終確認のために、すべての承認確認項目の承認が終了すると、文章選択手段１２５により記憶手段１３０に保存されている文章の中から所定の手順で最終承認用文章を選択し、端末装置２００に送信して端末装置２００のディスプレイ２３０に表示する処理と、該当個人がマイク２２３に向かって表示された文章を音読した音声の声紋情報を声紋照合手段１２３で記憶手段１３０の個人情報と照合して、該当個人の声紋であることを確認する処理と、該当個人がマイク２２３に向かって表示された文章を音読した音声の音声情報を音声照合手段１２４で文章選択手段１２５で選択された最終承認用文章と照合して、音声が最終承認用文章であることを確認する処理と、承認の最終確認のための声紋と音声とが確認されると、最終承認の成功メッセージを端末装置２００に送信しディスプレイ２３０に表示する処理と、次に防犯手段１２６で防犯動作が作動中か否かの確認を行って、防犯動作が作動していなければ、承認の最終確認が成功したものとして承認時に承認した電子承認をすべて完了させる処理と、を実行する。

【００３７】以上の処理から防犯キーワードを用いた防犯機能に関する処理が除かれていてもよい。

【００３８】

【発明の効果】以上説明したように、本発明においては、以下に記載するような効果を得ることができる。

【００３９】第１の効果は、認証時に生活反応を確認しているので、該当個人の遺体の一部（例えば眼球）を使用しただけでは、電子承認の作業まで進めず、電子承認が行えないことである。

【００４０】第２の効果は、電子承認の最終確認時に、該当個人の声紋照合と音声照合を行っているので、該当個人の音声の複製を用いては電子承認の最終確認が行えないことである。

【００４１】第３の効果は、「防犯キーワード認識によるセキュリティ機能」を採用しているので、該当個人以外の関与による操作を検知し、電子承認を無効にできることである。

【００４２】第４の効果は、「防犯キーワード認識によるセキュリティ機能」では正常終了と見せかけるので、該当個人への犯人からの脅迫を最低限に押さえることができることである。

【００４３】以上の効果が相乗されることにより、該当個人以外の関与による承認を確実に防止できるという効果がある。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態の個人識別を用いた電子承認システムの模式的ブロック構成図である。

【図２】認証時の各ステップを表すフローチャートである。

【図３】承認時の各ステップを表すフローチャートである。

【図４】承認の最終確認時の各ステップを表すフローチャートである。

【図５】防犯時の各ステップを表すフローチャートである。

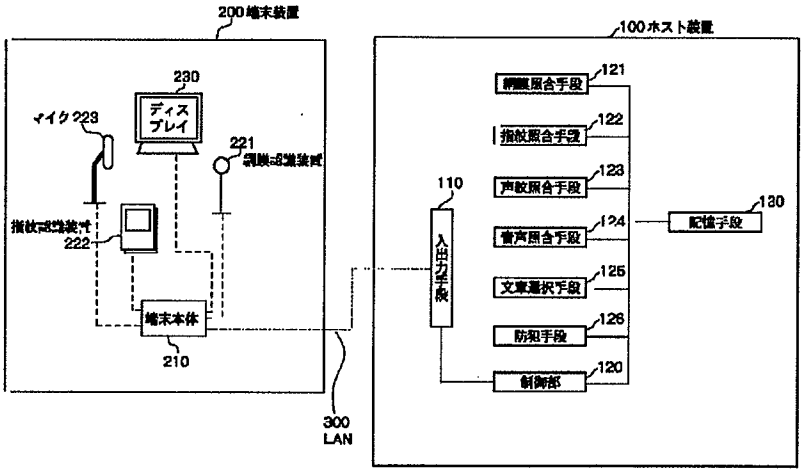
【図６】本発明の第２の実施の形態の個人識別を用いた電子承認システムの模式的ブロック構成図である。

【符号の説明】

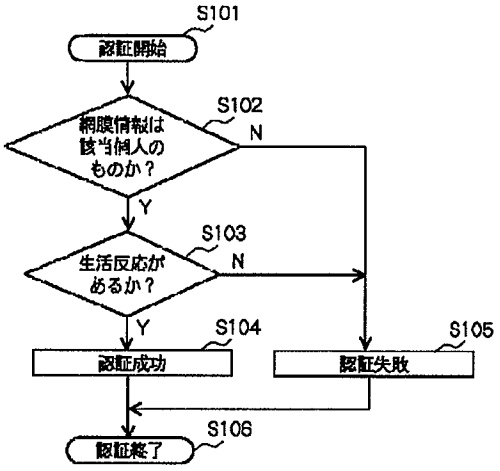
１００　ホスト装置
１０１　入力部
１０２　出力部
１０３　データ処理装置
１０４　記憶部
１０５　記録媒体
１１０　入出力手段
１２０　制御部
１２１　網膜照合手段

１２２	指紋照合手段	２２１	網膜認識装置
１２３	声紋照合手段	２２２	指紋認識装置
１２４	音声照合手段	２２３	マイク
１２５	文章選択手段	２３０	ディスプレイ
１２６	防犯手段	３００	ＬＡＮ
１３０	記憶手段	Ｓ１０１～１０６、Ｓ２０１～２０５、Ｓ３０１～Ｓ３１０、Ｓ４０１～Ｓ４０７	ステップ
２００	端末装置		
２１０	端末本体		

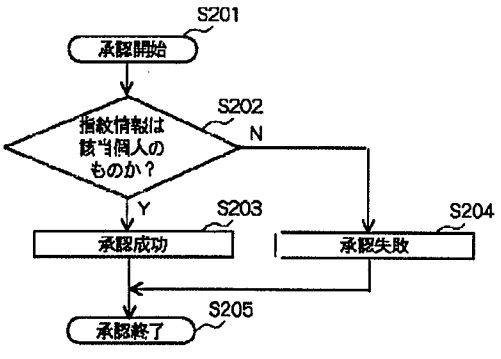
【図１】



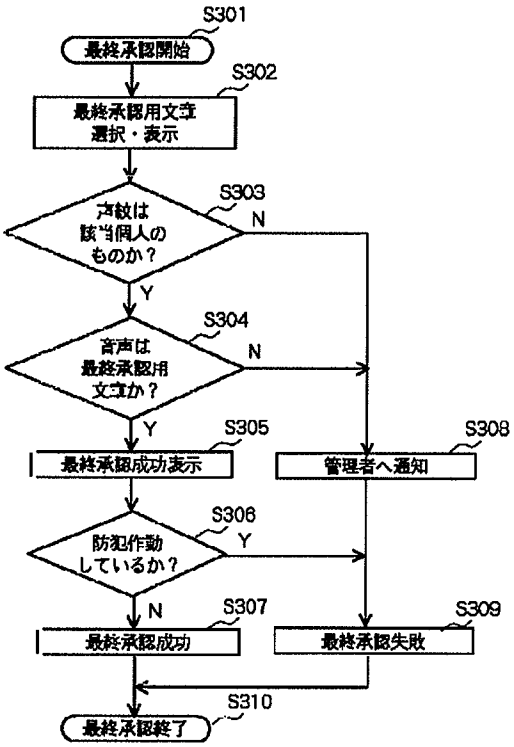
【図２】



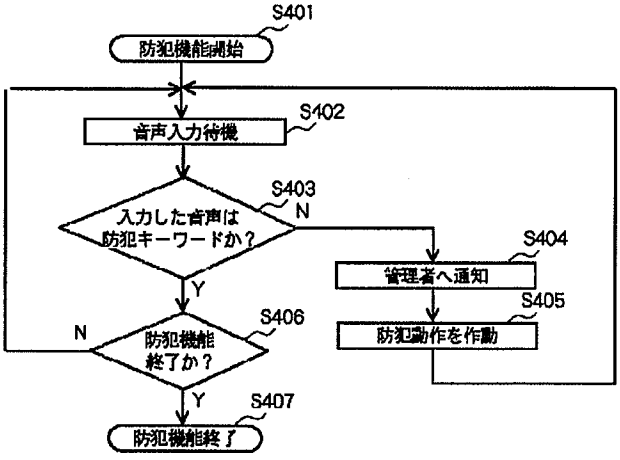
【図３】



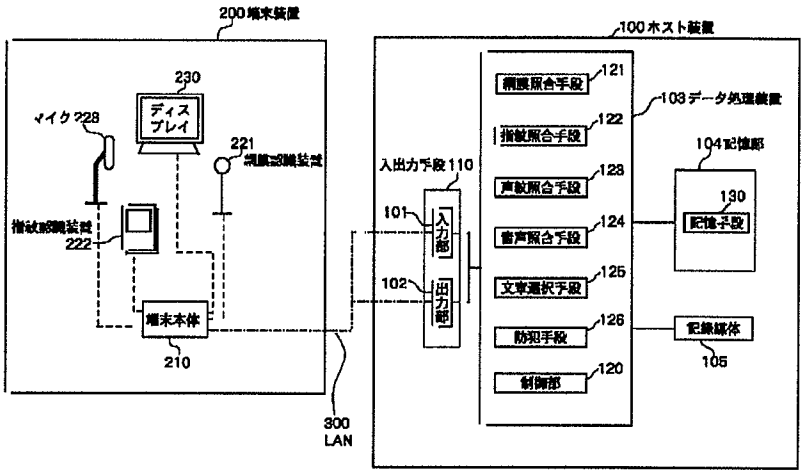
【図4】


S301
最終承認開始
S302
最終承認用文章
選択・表示
S303
声紋は
該当個人の
ものか？
N
Y
S304
音声は
最終承認用
文章か？
N
Y
S305
最終承認成功表示
S308
管理者へ通知
S306
防犯作動
しているか？
Y
N
S307
最終承認成功
S309
最終承認失敗
S310
最終承認終了

【図5】


S401
防犯機能開始
S402
音声入力待機
S403
入力した音声は
防犯キーワードか？
N
Y
S404
管理者へ通知
S405
防犯動作を作動
S406
防犯機能
終了か？
N
Y
S407
防犯機能終了

【図6】


200端末装置
230
ディスプレイ
マイク228
221
222
210
300
LAN
100ホスト装置
入出力手段110
101
入力部
102
出力部
121
122
123
124
125
126
120
103データ処理装置
104記憶部
130
記憶手段
記録媒体
105